Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 672 BRIEF VAN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 maart 2020

Tijdens het AO Digitale Overheid van 4 december jl. met de Minister van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 26 643, nr. 665) is uw Kamer naar aanleiding van vragen van het lid Özütok toegezegd met een schriftelijke reactie te komen op het rapport «Surveillance Giants: how the business model of Google and Facebook threatens human rights» van Amnesty International[1] en het rapport van de VN-rapporteur voor extreme armoede en mensenrechten van 11 oktober 2019 over de inzet van data-gedreven technologieën door overheden.[2] Ook is een schriftelijke reactie toegezegd op de vraag van het lid Verhoeven hoe om te gaan met de inzet van ingrijpende AI-toepassingen, zoals gezichtsherkenning, nu nog onduidelijk is of het wettelijk kader voor deze technologieën sluitend is. In deze brief doet de Minister van Binnenlandse zaken en Koninkrijksrelaties deze toezeggingen, samen met de Minister voor Rechtsbescherming en mede namens de Staatssecretaris van Economische Zaken en Klimaat, gestand.

Amnesty International rapport

Met veel interesse is kennisgenomen van het bovengenoemde rapport van Amnesty International. Het rapport beschrijft de dominante marktpositie van bedrijven als Google en Facebook in online dienstverlening en de verdienmodellen van deze bedrijven die leiden tot hun aanzienlijke datamacht. Het rapport beschrijft dat hierdoor niet alleen het recht op privacy onder druk komt te staan, maar ook vrijheidsrechten en het verbod van discriminatie. Amnesty International doet aanbevelingen aan overheden om dit tegen te gaan, zoals het versterken van regulering en toezicht.

[1] https://www.amnesty.org/en/documents/pol30/1404/2019/en/
[2] Report of the Special rapporteur on extreme poverty and human rights, Seventy-fourth session, item 72(b), 11 October 2019.

kst-26643-672
ISSN 0921 - 7371
’s-Gravenhage 2020

De door Amnesty International beschreven problematiek is al eerder geconstateerd, onder andere door het Rathenau Instituut in zijn rapport «Opwaarderen. Het borgen van publieke waarden in de digitale samenleving»[3] en door de Universiteit Utrecht in haar rapport «Algoritmes en grondrechten».[4] Het kabinet deelt de zorgen van deze organisaties en heeft in verschillende brieven zijn standpunten en beleid uiteen gezet.[5]
De juridische kaders voor de bescherming van mensenrechten zijn onder meer te vinden in de Grondwet, mensenrechtenverdragen, wetten zoals de Algemene Wet op de Gelijke Behandeling (AWGB) en Europese verordeningen zoals de Algemene Verordening Gegevensbescherming (AVG). Van belang is dat deze wetgeving onverkort in de online wereld van toepassing is en verplichtingen bevat waar bedrijven zoals Facebook en Google zich – ook in de digitale omgeving – aan moeten houden.
Hoewel deze wetten een robuust kader bieden voor de bescherming van mensenrechten, onderzoekt het kabinet of technologische ontwikkelingen ertoe leiden dat aanvullende wetgeving nodig is, bijvoorbeeld op het terrein van anti-discriminatie.[6] Daarnaast onderzoekt de Europese Commissie mogelijkheden voor aanvullende Europese wetgeving om mensenrechten bij AI-ontwikkelingen te borgen[7] en onderzoekt de Raad van Europa de haalbaarheid van een juridisch raamwerk voor AI-ontwikkelingen.[8]
In het kader van toezicht heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties afgelopen najaar onderzoek laten doen naar de wijze waarop toezicht op algoritmen bij de overheid is ingericht en hoe dit nog beter kan. Het onderzoek is in december jl. aan uw Kamer aangeboden[9] en een kabinetsreactie hierop volgt dit voorjaar. Wat betreft risicobeheersing door bedrijven refereerde het lid Özütok tijdens het AO aan de aanbeveling van Amnesty International om een bindende mensenrechtentoets te ontwikkelen voor het ontwerp, de toepassing en het gebruik van AI-systemen. Op dit moment verkent het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties de ontwikkeling van een mensenrechten impact assessment voor overheden, zodat overheden potentiële effecten van technologieën op mensenrechten in een vroegtijdig stadium in kaart kunnen brengen en kunnen adresseren. Te zijner tijd kan gekeken worden of dit mensenrechten impact assessment ook door bedrijven kan worden ingezet en het kabinet het gebruik hiervan kan stimuleren.
Amnesty International snijdt ook een belangrijk vraagstuk aan ten aanzien van de machtsposities van grote techbedrijven. Het kabinet deelt de analyse van Amnesty International en heeft al veel aandacht voor de macht van grote techbedrijven. De Staatssecretaris van EZK heeft in haar brief van 17 mei 2019[10] drie maatregelen voorgesteld om het mededingingsbeleid geschikt te maken om met de macht van grote techbedrijven om te gaan: (1) Een EU toezichthouder moet de mogelijkheid krijgen om vooraf maatregelen op te leggen aan platforms met een poortwachtersfunctie (of «gatekeepers» zoals Amnesty International deze platforms noemt; platforms waar consumenten en ondernemers niet of nauwelijks omheen kunnen) (2) voor effectieve handhaving van het mededingingstoezicht achteraf is aanpassing van de richtsnoeren nodig, zodat toezichthouders de beste methodes toepassen in hun handhaving en (3) introduceren van nieuwe concentratiedrempels zodat wanneer een machtig platform een potentiële concurrent of bedrijf met een waarde-

[3] https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen
[4] https://www.uu.nl/sites/default/files/rebo-montaigne-algoritmes_en_grondrechten.pdf
[5] Kamerstuk 26 643, nrs. 529, 601 en 642.
[6] Zoals aangekondigd in Kamerstuk 26 643, nr. 601.
[7] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf
[8] https://www.coe.int/en/web/artificial-intelligence/cahai
[9] Kamerstuk 26 643, nr. 657.
[10] Kamerstuk 27 879, nr. 71.

volle dataset wil opkopen, de overname onderhevig is aan beoordeling door een toezichthouder. De Staatssecretaris van EZK is in gesprek met andere lidstaten en met de Europese Commissie om steun voor de wijzigingen te verkrijgen. Reacties van andere lidstaten zijn overwegend positief en in de mission letter van Eurocommissaris Vestager, verantwoordelijk voor zowel mededinging als digitalisering, staat dat het mededingingsbeleid geschikt moet zijn voor de digitale samenleving. Bij haar hoorzitting in het Europees parlement verwees Vestager bovendien naar de Nederlandse inzet.

VN rapport

Daarnaast is met veel interesse kennisgenomen van het bovengenoemd rapport van de VN-rapporteur voor extreme armoede en mensenrechten. Het rapport beschrijft de opkomst van de digitale verzorgingsstaat, waarin sociale bescherming en diensten steeds meer vorm krijgen via data-gedreven technologieën. Bij voorspellingen op basis van data/AI bestaat het risico dat bestaande bias in data en/of beleid wordt gereproduceerd. De Minister van Binnenlandse Zaken en Koninkrijksrelaties beschreef zijn zorgen omtrent het risico op benadeling van groepen in verschillende Kamerbrieven, alsook het beleid dat hierop ontwikkeld wordt.[11] Voorop staat dat ongerechtvaardigde ongelijke behandeling op basis van verdachte kenmerken (zoals etniciteit, geslacht of leeftijd) krachtens de Grondwet verboden is, ook als dit online gebeurt. Dit verbod is uitgewerkt en/of verder gespecificeerd in andere wetten en verordeningen zoals de AWGB en de AVG. Daarnaast is transparantie over datagebruik en AI-inzet van belang. Eerder zette de Minister voor Rechtsbescherming het kabinetsbeleid op het gebied van transparantie van overheidsalgoritmen uiteen[12] en ontwikkelde hij richtlijnen voor het toepassen van algoritmen door overheden, waaronder richtlijnen voor publieksvoorlichting over data-analyses.[13] Ook de rechter benadrukte onlangs het belang van transparantie in een gerechtelijke uitspraak over het Systeem Risico Indicatie (SyRI).[14] Nieuwe technologieën zoals AI of de inzet van technologische concepten zoals «big data» kunnen ertoe leiden dat bestaande wettelijke kaders verder aangescherpt moeten worden om te voorkomen dat benadeling van groepen of individuen plaatsvindt. Daarom onderzoekt het kabinet zoals boven vermeld of aanvullende wetgeving nodig is op het terrein van anti-discriminatie en, meer in het algemeen, of aanvullende wettelijke waarborgen tegen de risico's van data-analyse[15] nodig zijn. Daarnaast ontwikkelt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een mensenrechten impact assessment om risico's op o.a. discriminatie vroegtijdig in kaart te brengen en te mitigeren. Ook ontwikkelt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties principes voor systeemontwikkelaars om discriminatie door AI-systemen te voorkomen.

Gezichtsherkenning

Het lid Verhoeven stelde tijdens bovengenoemd AO de vraag hoe het kabinet omgaat met de toepassing van gezichtsherkenningscamera's in allerlei praktijksituaties, terwijl momenteel nog onduidelijk is of het wettelijk kader voor de toepassing van deze technologie wel sluitend is. Belangrijk hierbij is dat er voor de verwerking van biometrische persoons-

[11] Kamerstuk 26 643, nrs. 529, 601 en 642.
[12] Kamerstuk 26 643, nr. 570.
[13] Zie bijlage bij Kamerstuk 26 643, nr. 641.
[14] Uitspraak Rechtbank De Haag inzake Syri 5 februari 2020. De Staatssecretaris van SZW zal in een Kamerbrief op de uitspraak ingaan.
[15] Kamerstuk 26 643, nr. 641.

gegevens[16] een uitgebreid kader is, dat strenger is dan bij de verwerking van gewone persoonsgegevens. Dat kader is onder meer neergelegd in de AVG en de Uitvoeringswet AVG (UAVG), welke zowel op overheden[17] als bedrijven van toepassing zijn.

De AVG regelt dat het verwerken van biometrische gegevens in beginsel verboden is (art. 9 lid 1).[18] Hierop is een aantal rechtsgronden voor uitzondering geformuleerd (art. 9 lid 2). Eén daarvan is de uitdrukkelijke toestemming door betrokkene voor de verwerking van de biometrische persoonsgegevens voor welbepaalde doeleinden. De AVG bepaalt (art. 4 lid 11) dat de toestemming van een betrokkene moet zijn gebaseerd op een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt. Dit betekent bijvoorbeeld dat toestemming alleen plaats kan vinden als de betrokkene een werkelijke keuze heeft en dat toestemming in bepaalde gezagsverhoudingen (zoals tussen werkgever en werknemer) zelden een passende grondslag is.
Daarnaast kan het verwerken van biometrische gegevens toegestaan zijn als dit noodzakelijk is om redenen van zwaarwegend algemeen belang, dit bij nationale wet geregeld is en aan specifieke waarborgen wordt voldaan. In de Uitvoeringswet AVG is van de regeling via nationale wet gebruik gemaakt door te bepalen dat het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken, niet van toepassing is, indien deze verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden (art. 29). Deze grondslag kan bijvoorbeeld gebruikt worden voor het instellen van een op gezichtsherkenning gebaseerde toegang tot een locatie, zoals een gebouw. Bij noodzakelijkheid van een verwerking moet voldaan zijn aan het proportionaliteits- en het subsidiariteitsbeginsel. Proportionaliteit vereist dat het doel in verhouding staat tot de inbreuk die wordt gemaakt en subsidiariteit dat het doel niet op een minder nadelige manier kan worden bereikt.[19]
Tijdens het AO signaleerde het lid Verhoeven terecht dat de afweging of gezichtsherkenning met behulp van camera's toelaatbaar is, sterk verschilt per situatie en context. Voordat gezichtsherkenning met behulp van camera's wordt ingezet, moet onder andere altijd zorgvuldig gekeken worden wat het doel van de inzet van de technologie is, wat de nauwkeurigheid van de technologie is, welke voor- en nadelen de technologie kent, of er inbreuk gemaakt wordt op de private sfeer, hoe deze aspecten in verhouding staan tot het doel en of het doel op andere wijze kan worden bereikt. Er kunnen situaties bij de inzet van de technologie ontstaan, waarvoor in zijn algemeenheid gevonden wordt dat de inzet van de

---

[16] Biometrische persoonsgegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon. Op grond hiervan is eenduidige identificatie van die persoon mogelijk. Of wordt zijn/haar identiteit bevestigd.

[17] Wanneer een overheid biometrische gegevens verwerkt dan geldt aanvullende nationale en internationale wetgeving, zoals de Paspoortwet, de Schengengrenscode en de Wet politiegegevens. In november 2019 stuurde de Minister van Justitie en Veiligheid een brief naar uw Kamer over waarborgen en kaders bij gebruik van gezichtsherkenningstechnologie door de overheid (met name veiligheidsinstanties zoals de politie), Kamerstuk 32 761, nr. 152.

[18] De AVG is niet van toepassing op verwerking in het kader van zuiver persoonlijke of huishoudelijke activiteiten. Er is sprake van zuiver persoonlijke of huishoudelijk activiteiten wanneer een individu persoonsgegevens alleen voor privédoeleinden gebruikt en dit gebruik niet samenhangt met zakelijke activiteiten. In relatie tot biometrische gegevens is het ontgrendelen van een smartphone met behulp van gezichtsherkenning hier een voorbeeld hiervan.

[19] Bij alle gegevensverwerkingen, dus ook bij de uitzonderingen op het verbod van biometrische gegevensverwerking, moet altijd voldaan zijn aan de basis beginselen van de AVG (overweging 39). Deze beginselen zijn vastgelegd in verschillende artikelen en omvatten bijvoorbeeld rechtmatigheid, behoorlijkheid, transparantie, verantwoordelijkheid en juistheid (zie art. 5).

technologie in principe niet toelaatbaar is. Hier kan indien nodig aanvullende regelgeving op plaatsvinden. Het kabinet laat door het WODC onderzoek doen met als doelstelling om meer inzicht te krijgen in de wijze waarop het gebruik van gezichtsherkenningstechnologie inbreuk kan maken op de privacy. Dit onderzoek zal voor de zomer van 2020 aan uw Kamer worden toegezonden. Daarnaast wordt er door de Minister voor Rechtsbescherming gewerkt aan een Kamerbrief over de feitelijke toepassingen van gezichtsherkenning in Nederland en het juridische kader dat daarop van toepassing is.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

De Minister voor Rechtsbescherming,
S. Dekker